

Mark L. Smith (#14762)
msmith@smithwashburn.com
SMITH WASHBURN, LLP
 6871 Eastern Avenue., Suite 101
 Las Vegas, NV 89119
 Telephone: (725) 666-8701
 Facsimile: (725) 666-8710

Attorneys for Reflex Media, Inc.

IN THE UNITED STATES DISTRICT COURT
 DISTRICT OF NEVADA

REFLEX MEDIA, INC., a Nevada
 Corporation,

 Plaintiff,

 v.

 AARON WALLACE, an individual, *et al.*,

 Defendant.

Case No. 2:18-cv-02423-RFB-PAL

**OPPOSITION TO WEB PRESENCE LLC'S
 MOTION TO DISMISS PLAINTIFF'S SECOND
 AMENDED COMPLAINT**

Plaintiff Reflex Media, Inc. ("Reflex"), by and through its counsel of record, hereby respectfully submits the following Memorandum of Points and Authorities in opposition to Defendant Web Presence, LLC's Motion to Dismiss Plaintiff's Second Amended Complaint ("Motion" or "Motion to Dismiss").

Reflex Media's opposition is based upon the following Memorandum of Points and Authorities, the papers attached thereto, the papers and pleadings on file with the Court, the concurrently filed Motion to Strike Assertions of Fact From Web Presence's Motion to Dismiss ("Motion to Strike") and Evidentiary Objections to Evidence Offered in the Declaration of Bryan Mendes in Support of Opposition To Web Presence LLC's Motion To Dismiss Plaintiff's Second Amended Complaint ("Evidentiary Objections"), and any oral argument the Court may entertain concerning this matter.

////

////

////

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Procedural Facts.....	3
III.	Pleading Standards.....	3
IV.	Argument	6
	(a) Reflex Has Sufficiently Alleged that Web Presence Participated in the Wrongful Act of Extortion.	6
	(1) Web Presence’s Alleged Misconduct Falls Squarely Within <i>Bollaert</i> and Sufficiently Pleads that Web Presence Engaged in the Extortion that Injured Reflex.	6
	(2) The Communication Decency Act Provides No Protection for Web Presence.....	7
	(b) Web Presence is a Knowing and Willing Participant in the Extortion Scheme Conspiracy.	11
	(c) The Second Amended Complaint is Sufficiently Clear as to the Roles of Each Extortion Scheme Participant.	13
	(d) Extortion Scheme Participants Violated the Computer Fraud and Abuse Act, Giving This Court Subject Matter Jurisdiction, and California Penal Code §502.....	14
	(1) Reflex Has Made Numerous and Detailed Allegations Relating to Computer Crimes, Including the Following	14
	(2) Defendants’ Unlawful Access Gives Rise to a Sufficiently Pled and Valid CFAA Claim....	15
	(3) Defendants’ Unpermitted Access is Sufficiently Pleaded to State a Valid Cause of Action Under California Penal Code § 502.....	17
	(e) Reflex Successfully Pled Intentional and Negligent Interference with Prospective Economic Advantage, And Unfair Competition Causes of Action	18
	(f) Reflex Does not Rely upon Fraud to State its Causes of Action	19
	(g) Reflex’s Detailed Pleadings Easily Satisfy the Pleading Standard Set Forth in <i>Twombly</i>	20
	(h) Reflex May Bring Claims Based on the Law of Other Forums.	23
	(i) The Northern District of California Has Already Found that This Court Has Subject Matter Jurisdiction, Personal Jurisdiction, and is a Proper Venue for this Case.....	24

V. Conclusion 24

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF AUTHORITIES

CASES

<i>Arista Records, LLC v. Doe 3</i> , 604 F.3d 110 (2d Cir. 2010)	5
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009).....	5
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007).....	5, 21, 22
<i>Bristol-Myers Squibb Co. v. Superior Court of California, San Francisco Cty.</i> , 137 S. Ct. 1773, 198 L. Ed. 2d 395 (2017)	23
<i>BriteSmile, Inc. v. Discus Dental, Inc.</i> , No. C 02-03220 JSW, 2005 WL 3096275 (N.D. Cal. Nov. 18, 2005)	19
<i>Butler v. Los Angeles Cty.</i> , 617 F. Supp. 2d 994 (C.D. Cal. 2008)	14
<i>Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.</i> , 20 Cal. 4th 163 (1999)	18
<i>Cicone v. URS Corp.</i> , 183 Cal. App. 3d 194 (Ct. App. 1986).....	4
<i>City & Cty. of San Francisco v. Philip Morris, Inc.</i> , 957 F. Supp. 1130 (N.D. Cal. 1997)	4, 20
<i>Clegg v. Cult Awareness Network</i> , 18 F.3d 752 (9th Cir. 1994)	6
<i>Concha v. London</i> , 62 F.3d 1493 (9th Cir. 1995)	5
<i>de Vries v. Brumback</i> , 349 P.2d 532 (1960).....	12, 13
<i>Duncan v. Stuetzle</i> , 76 F.3d 1480 (9th Cir. 1996)	19
<i>E. & J. Gallo Winery v. F. & P. S.p.A.</i> , 899 F. Supp. 465 (E.D. Cal. 1994)	24
<i>eBay Inc. v. Digital Point Sols., Inc.</i> , 608 F. Supp. 2d 1156 (N.D. Cal. 2009)	19
<i>Facebook, Inc. v. MaxBounty, Inc.</i> , 274 F.R.D. 279 (N.D.Cal.2011).....	19
<i>Facebook, Inc. v. Power Ventures, Inc.</i> , 844 F.3d 1058 (9th Cir. 2016)	16, 17, 18

1	<i>Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC</i> ,	9
2	521 F.3d 1157 (9th Cir. 2008).....	
3	<i>Flatley v. Mauro</i> ,	6
4	139 P.3d 2 (Cal. 2006)	
5	<i>Gilbrook v. City of Westminster</i> ,	11
6	177 F.3d 839 (9th Cir. 1999)	
7	<i>Gilligan v. Jamco Dev. Corp.</i> ,	5
8	108 F.3d 246 (9th Cir. 1997)	
9	<i>Hall v. City of Santa Barbara</i> ,	5
10	833 F.2d 1270 (9th Cir.1986)	
11	<i>Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc.</i> ,	20
12	556 F. Supp. 2d 1122 (E.D. Cal. 2008)	
13	<i>In re Carrier IQ, Inc.</i> ,	18
14	78 F. Supp. 3d 1051 (N.D. Cal. 2015)	
15	<i>Keeton v. Hustler Magazine, Inc.</i> ,	23
16	465 U.S. 770, 104 S. Ct. 1473, 79 L. Ed. 2d 790 (1984).....	
17	<i>Korea Supply Co. v. Lockheed Martin Corp.</i> ,	18
18	29 Cal. 4th 1134, 63 P.3d 937 (2003)	
19	<i>Levitt v. Yelp! Inc.</i> ,	7, 8, 18
20	765 F.3d 1123 (9th Cir. 2014)	
21	<i>Lucas v. Dep't of Corr.</i> ,	6
22	66 F.3d 245 (9th Cir. 1995)	
23	<i>McGraw Co. v. Aegis Gen. Ins. Agency, Inc.</i> ,	4
24	No. 16-CV-00274-LB, 2016 WL 3745063 (N.D. Cal. July 13, 2016)	
25	<i>Mirkin v. Wasserman</i> ,	4, 20
26	858 P.2d 568 (Cal. 1993)	
27	<i>Multiven v. Cisco</i> ,	20
28	725 F.Supp.2d 887 (N.D.Cal.2010)	
	<i>Musacchio v. United States</i> ,	16
	136 S.Ct. 709, 193 L.Ed.2d 639 (2016)	
	<i>N. Am. Chem. Co. v. Superior Court</i> ,	18
	59 Cal. App. 4th 764, 69 Cal. Rptr. 2d 466 (1997).....	
	<i>NetApp, Inc. v. Nimble Storage, Inc.</i> ,	19
	41 F. Supp. 3d 816 (N.D. Cal. 2014)	
	<i>Oracle Am., Inc. v. TERiX Computer Co., Inc.</i> ,	4
	No. 5:13-CV-03385-PSG, 2014 WL 31344 (N.D. Cal. Jan. 3, 2014)	
	<i>Oracle Am., No. 5:13-CV-03385-PSG</i> ,	20
	2014 WL 31344 (N.D. Cal. Jan. 3, 2014)	

1	<i>Park v. Thompson</i> , 851 F.3d 910 (9th Cir. 2017)	5, 20, 21
2	<i>People v. Bollaert</i> , 248 Cal. App. 4th 699 (2016)	passim
3		
4	<i>Prop. Rights Law Grp., P.C. v. Lynch</i> , No. 13–00273, 2013 WL 4791485 (D.Haw. Sep. 16, 2013)	19
5	<i>Retiree Support Grp. of Contra Costa Cty. v. Contra Costa Cty.</i> , 944 F. Supp. 2d 799 (N.D. Cal. 2013)	6
6		
7	<i>Robertson v. Dean Witter Reynolds, Inc.</i> , 749 F.2d 530 (9th Cir.1984)	3
8	<i>Saunders v. Superior Court</i> , 27 Cal. App. 4th 832 (1994)	18
9		
10	<i>SmileCare Dental Group v. Delta Dental Plan of Cal., Inc.</i> , 88 F.3d 780 (9th Cir. 1996)	3
11	<i>Smith & Hawken, Ltd. v. Gardendance, Inc.</i> , 2004 WL 2496163, 2004 Copr. L. Dec. P 28,903	19
12		
13	<i>SuccessFactors, Inc. v. Softscape, Inc.</i> , 544 F. Supp. 2d 975 (N.D. Cal. 2008)	17
14	<i>Synthes, Inc. v. Knapp</i> , 250 F. Supp. 3d 644 (E.D. Cal. 2017)	23
15		
16	<i>Thermolife Int'l, LLC v. Vital Pharm., Inc.</i> , No. CV142449RSWLAGRX, 2014 WL 12235190 (C.D. Cal. Aug. 15, 2014).....	24
17	<i>Ticketmaster L.L.C. v. Prestige Entm't W., Inc.</i> , 315 F. Supp. 3d 1147 (C.D. Cal. 2018)	15, 16
18		
19	<i>United States v. Christensen</i> , 801 F.3d 970 (2015).....	18
20	<i>United States v. Ritchie</i> , 342 F.3d 903 (9th Cir. 2003)	5
21		
22	<i>Vess v. Ciba–Geigy Corp. USA</i> , 317 F.3d 1097 (9th Cir.2003)	4, 20
23	<i>Vieux v. East Bay Reg'l Park Dist.</i> , 906 F.2d 1330 (9th Cir.1990)	11
24		
25	<i>World Health & Educ. Found. v. Carolina Cas. Ins. Co.</i> , 612 F. Supp. 2d 1089 (N.D. Cal. 2009)	5, 20
26	<i>Wyatt v. Union Mortg. Co.</i> , 598 P.2d 45 (1979).....	11, 22
27		
28		

STATUTES

1	18 USC § 1030 <i>et seq.</i>	17
2	28 U.S.C. § 1331.....	17
3	28 U.S.C. § 1367.....	17
4	47 U.S.C. § 230 (f)(3)	8, 9
5	47 U.S.C. § 230(c)(1).....	8
6	Cal. Penal Code § 519.....	7
7	Cal. Penal Code § 523.....	7
8	Cal. Penal Code §518.....	6, 7

OTHER AUTHORITIES

10	Gene Zorkin, “Sugar Dating” Site Sues Over Alleged Extortion of its Members, YNOT (Aug. 21, 2018),	
11	https://www.ynot.com/sugar-dating-site-sues-extortion-members/ (last visited Nov. 15, 2018).....	10

MEMORANDUM OF POINTS AND AUTHORITIES**I. INTRODUCTION**

Plaintiff Reflex Media, Inc. (“Reflex”) wishes to end an extortion scheme that includes Defendant Web Presence among its perpetrators. Reflex’s Second Amended Complaint (the “SAC” at ECF No. 84) has more than adequately alleged Web Presence’s role in that scheme.¹ This is reinforced by the fact that Web Presence’s Motion to Dismiss (ECF No. 92) doesn’t argue the adequacy of Reflex’s allegations so much as it attempts to refute them with an untimely, inappropriate, and evidentiarily defective declaration. Accordingly, on the basis of the Reflex’s arguments herein, Web Presence’s Motion to Dismiss should be denied, or, on the basis of the improper introduction of evidence, the Motion should be converted to a motion for summary judgment.

The case against Web Presence is simple and straightforward. The scheme alleged is extortion and blackmail, with Web Presence filling the role of payment processor and money changer. Data Miners start by creating profiles on SeekingArrangement.com and harvesting the personal information of Reflex’s customers’ (the “SA Members”). The SA Members’ personal information is then posted on the Extortion Websites.² Removal from these sites is only possible by paying other websites that have been pre-arranged to provide such a service. Web Presence is one of these sites that take money from extortion victims and splits it with the Extortion Websites.

The case against Web Presence is even stronger than just that, however. Web Presence actually interacts with the victims, sets the extortion price for removal, and makes the implicit threat through these communications that failure to pay will result in having the extortive information remain online. Specifically, Web Presence, in exchange for hundreds or thousands of dollars per person, cleared names from the Extortion Websites and paid those Extortion Websites (often through clandestine payment systems like Bitcoin) for the removal, less the amount pocketed by Web Presence. (See Reflex’s SAC at ¶3 (describing the Extortion Scheme).)³ This all by itself constitutes extortion with Web Presence as a primary participant under California precedent affirming the criminal conviction of a man who had

¹ The term “Web Presence,” as used here, includes Web Presence LLC d/b/a www.EraseMugShots.com, www.NetReputation.com, www.GuaranteedRemoval.com, www.ReputationLawyers.com and www.RemoveMugshots.net.

² The Extortion Websites here include PredatorsAlert.com, PredatorAlerts.com, PredatorsAlerts.com, PredatorAlerts.co, and PredatorExposed.com.

³ This service was also performed by Defendant Marca Global, LLC d/b/a www.InternetReputation.com (“Marca” and together with Web Presence, the “Removal Sites” or “Removal Websites”).

engaged in virtually identical behavior. *See People v. Bollaert*, 248 Cal. App. 4th 699 (2016). In fact, the *Bollaert* decision alone disposes most of Web Presence’s arguments here. *See id.* at 710 (rejecting proffered defense that “it was the third parties ... who submitted the personal information and he [the defendant] maintains he only provided the opportunity for third parties to post the information of their choice.”); *id.* at 722 (rejecting defendant’s argument that “he was under no legal obligation to remove third party postings from his Web site ...but instead merely offered a service to remove the photos,” this being “standard business practice” as opposed to extortion.)

Here, Web Presence actually admits that it took money to clear people’s names off of the Extortion Websites and does not deny that it split that money with the Extortion Websites for doing so. (*See* Web Presence’s Motion to Dismiss (ECF No. 92) at pp. 2–3.) As a result, Web Presence can’t deny that it (1) set the prices for content removal, (2) took the money from the victims, (3) arranged with the Extortion Websites for the content to come down permanently, (4) without any negotiation or requirement of proof of falsehood, and (5) paid the Extortion Websites, (6) often converting the dollars they received into bitcoin to assist in making the funds difficult to trace, for doing so. (*See* SAC at (ECF No. 84) at ¶¶ 3, 23 70–72, 74); Motion to Dismiss (ECF No. 92) at 2–3.) Web Presence, therefore, also cannot deny its essential role in the Extortion Scheme and that its actions constitute extortion under *Bollaert* and other governing legal authority. This is important not because Reflex has sued Web Presence for extortion directly (it has not), but because the Extortion Scheme constitutes the wrongful act that forms the predicate for several of Reflex’s state law claims (although extortion is not a required predicate for Reflex’s federal Computer Fraud and Abuse Act (“CFAA”) claim).

Web Presence also cannot claim ignorance as to the effects of its actions on Reflex. Web Presence knew that the information it was being paid to remove came from SeekingArrangement.com member profiles, because the victims who were paying for content removal ***told the payment sites like Web Presence that this was where the information came from.*** (SAC (ECF No. 84) at ¶¶ 95, 103.) Hence, Web Presence knew that Reflex was as much of a victim of the Extortion Scheme as were the desperate individuals whom Web Presence charged for content removal.

Web Presence cannot evade Reflex’s specific allegations with a declaration of cherry-picked facts that is wholly inappropriate on a motion to dismiss (this is the subject of Reflex’s Motion to Strike and

Evidentiary Objections filed concurrently herewith). That being said, it is instructive to observe what facts Web Presence does *not* deny, even in its own improper declaration. (*See* Mendes Declaration (ECF No. 92-1).) Web Presence does not deny that it took money to remove personal names and information from the Extortion Websites, that it paid some of that money to the Extortion Websites—perhaps in Bitcoin or otherwise clandestinely—that it communicated with at least some Extortion Website operators, or that it performed these services for SeekingArrangement.com members. Unable to deny even these basic elements of participation in the Extortion Scheme, Web Presence cannot prevail at any stage of the case, much less here where this Court must accept Reflex’s well-pled allegations.

Reflex has, therefore, more than adequately alleged enough to survive a motion to dismiss, and has specifically and adequately alleged that (1) Web Presence’s actions constitute extortion under California law and therefore serve as the predicate for other claims under California law; (2) Web Presence willingly participated in the Extortion Scheme against people they knew were SA’s Members directly, and as a co-conspirator, and is liable for all acts by all other participants in that scheme, including violations of the Computer Fraud and Abuse Act and California Penal Code § 502; and (3) Web Presence has violated the CFAA and all other relevant statutes. Accordingly, this Court should deny Web Presence’s Motion to Dismiss.

II. PROCEDURAL FACTS

1. This Case was originally filed in the Northern District of California. (*See* ECF No. 1).

2. On December 21, 2018, Judge Hamilton partially granted Defendant Marca’s motion to transfer and transferred the case to this Court pursuant to 28 U.S.C. § 1404(a), finding that “this action could have originally been brought in the United States District Court for the District of Nevada”. (*See* ECF No. 61, Order Granting in Part Defendant’s Motion to Transfer, hereinafter, the “Transfer Order”).

III. PLEADING STANDARDS

Under Rule 12(b)(6) a court may dismiss a complaint for “(1) lack of a cognizable legal theory; or (2) insufficient facts under a cognizable legal theory.” *SmileCare Dental Group v. Delta Dental Plan of Cal., Inc.*, 88 F.3d 780, 783 (9th Cir. 1996) (citing *Robertson v. Dean Witter Reynolds, Inc.*, 749 F.2d 530, 534 (9th Cir.1984)). When considering a motion to dismiss, “[a]ll allegations of material fact in the

complaint are taken as true and construed in the light most favorable to the plaintiff.” *Id.* (citing *Everest & Jennings v. American Motorists Ins. Co.*, 23 F.3d 226, 229 (9th Cir.1994)).

Although Web Presence argues that Reflex’s entire SAC must be evaluated under Rule 9(b), Rule 9(b)’s heightened pleading standards only apply to (1) actual allegations of fraud, and (2) an entire claim where a plaintiff alleges a “unified course of conduct” and relies “entirely on that course of conduct as the basis of a claim.” *Vess v. Ciba–Geigy Corp. USA*, 317 F.3d 1097, 1102–06 (9th Cir.2003) (internal quotation marks omitted). The elements of fraud are: “(1) misrepresentations; (2) knowledge of falsity; (3) intent to defraud, i.e., intent to induce reliance; (4) justifiable reliance [by the person defrauded]; and (5) resulting damage.” *City & Cty. of San Francisco v. Philip Morris, Inc.*, 957 F. Supp. 1130, 1141 (N.D. Cal. 1997) (citing *Cicone v. URS Corp.*, 183 Cal. App. 3d 194, 200, (Ct. App. 1986)). Importantly, “[a] plaintiff must plead that he or she actually relied on the misrepresentation” to constitute an allegation of fraud. *Id.* (citing *Mirkin v. Wasserman*, 858 P.2d 568, 570 (Cal. 1993)).

And even if “a plaintiff may choose [...] to allege some fraudulent and some non-fraudulent conduct [...] ***only the allegations of fraud are subject to Rule 9(b)'s heightened pleading requirements.***” *Vess*, 317 F.3d at 1104 (emphasis added). Rule 9(b) “does not require that allegations supporting a claim be stated with particularity when those allegations describe non-fraudulent conduct ... ***[t]o require that non-fraud allegations be stated with particularity merely because they appear in a complaint alongside fraud averments, [...] would impose a burden on plaintiffs not contemplated by the notice pleading requirements of Rule 8(a).***” *Vess*, 317 F.3d at 1104 (emphasis added); see *McGraw Co. v. Aegis Gen. Ins. Agency, Inc.*, No. 16-CV-00274-LB, 2016 WL 3745063, at *2 (N.D. Cal. July 13, 2016) (finding that even where averments of fraud are present in a complaint, Rule 9(b) “does not require [] plaintiffs to plead every fact and claim with heightened particularity”). Finally, claims made under the Computer Fraud and Abuse Act do not invoke the pleading requirements under Rule 9(b). *Oracle Am., Inc. v. TERiX Computer Co., Inc.*, No. 5:13-CV-03385-PSG, 2014 WL 31344, at *5 (N.D. Cal. Jan. 3, 2014) (finding that Rule 9(b) pleading standards do not apply to CFAA allegations where a plaintiff does not rely on a misrepresentation by a defendant, even if its customers did).

When considering allegations in the complaint (that do not concern fraud), the “court does not require heightened fact pleading of specifics;” it only requires “***enough facts to state a claim to relief***

1 ***that is plausible on its face.***” *World Health & Educ. Found. v. Carolina Cas. Ins. Co.*, 612 F. Supp. 2d
 2 1089, 1093 (N.D. Cal. 2009) (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570, 127 S.Ct. 1955,
 3 1974, 167 L.Ed.2d 929 (2007) (internal quotations omitted, emphasis added). A court should consider
 4 the entire factual conduct alleged in a complaint to analyze whether a plaintiff has “[nudged its claim]
 5 across the line from conceivable to plausible.” *See Soo Park v. Thompson*, 851 F.3d 910, 928 (9th Cir.
 6 2017), *cert. denied sub nom. Thompson v. Park*, 138 S. Ct. 642, 199 L. Ed. 2d 527 (2018) citing
 7 *Ashcroft v. Iqbal*, 556 U.S. 662, 680, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009) (internal quotation marks
 8 omitted) “The *Twombly* plausibility standard ... ***does not prevent a plaintiff from pleading facts alleged***
 9 ***upon information and belief where the facts are peculiarly within the possession and control of the***
 10 ***defendant or where the belief is based on factual information that makes the inference of culpability***
 11 ***plausible.***” *Id.* (citing *Arista Records, LLC v. Doe 3*, 604 F.3d 110, 120 (2d Cir. 2010) (emphasis
 12 added)); *see also Concha v. London*, 62 F.3d 1493, 1503 (9th Cir. 1995) (“***[W]e relax pleading***
 13 ***requirements where the relevant facts are known only to the defendant.***”) (emphasis added).

14 Moreover, “[a] court may [...] consider certain materials—documents attached to the complaint,
 15 documents incorporated by reference in the complaint, or matters of judicial notice” when reviewing a
 16 12(b)(6) motion. *United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003).” However, “[w]hen ruling
 17 on a Rule 12(b)(6) motion to dismiss, ***if a district court considers evidence outside the pleadings, it***
 18 ***must normally convert the 12(b)(6) motion into a Rule 56 motion for summary judgment [...]***”⁴ *Id.*
 19 (emphasis added).

20 As a general matter, “[m]otions to dismiss generally are viewed with disfavor and are to be granted
 21 rarely.” *Gilligan v. Jamco Dev. Corp.*, 108 F.3d 246, 249 (9th Cir. 1997)) (quoting *Hall v. City of Santa*
 22 *Barbara*, 833 F.2d 1270, 1274 (9th Cir.1986)). Accordingly, “[a] complaint should not be dismissed
 23 unless it appears beyond doubt the plaintiff can prove no set of facts in support of his claim that would

24 _____
 25 ⁴ Web Presence goes beyond the pleadings by introducing a declaration and making several factual
 26 averments in its Motion. It has also has actually fabricated allegations that it says are in the SAC that
 27 simply are not. For example, Web Presence states in its Motion, “The allegations in the SAC, insofar as
 28 they pertain to Web Presence, are two people contacted Web Presence and paid for content removal, which
 was done successfully. These people who contacted Web Presence did not identify themselves as
 SeekingArrangement.com members, or that there was anything unusual about their removal requests.”
 (ECF No. 92 at 2:23-26) To the extent that it purports to introduce new “facts,” those facts are also without
 any factual basis and immaterial on the applicable standard here. Reflex requests that such out-of-
 pleadings factual assertions be stricken, or (in the alternative), that Web Presence’s Motion to Dismiss be
 converted to a motion for summary judgment.

entitle him to relief.” *Clegg v. Cult Awareness Network*, 18 F.3d 752, 754 (9th Cir. 1994). And even then, “leave to amend must be granted unless it is clear that the complaint’s deficiencies cannot be cured by amendment.” *Retiree Support Grp. of Contra Costa Cty. v. Contra Costa Cty.*, 944 F. Supp. 2d 799, 803 (N.D. Cal. 2013) (citing *Lucas v. Dep’t of Corr.*, 66 F.3d 245, 248 (9th Cir. 1995)).

IV. ARGUMENT

(a) REFLEX HAS SUFFICIENTLY ALLEGED THAT WEB PRESENCE PARTICIPATED IN THE WRONGFUL ACT OF EXTORTION.

(1) Web Presence’s Alleged Misconduct Falls Squarely Within *Bollaert* and Sufficiently Pleads that Web Presence Engaged in the Extortion that Injured Reflex.

Reflex has adequately alleged extortion, which—though not a claim that Reflex has brought—is nonetheless a predicate for some of Reflex’s state law claims (although not the federal CFAA cause of action). Extortion “is the [act of] obtaining of property from another, with his consent ... induced by a wrongful use of force or fear....” Cal. Penal Code §518. “Fear, for purposes of extortion “may be induced by a threat of any of the following: [¶] ... [¶] ... To accuse the individual threatened ... of a crime”; or “[t]o expose, or impute to him ... a deformity, disgrace or crime” or “expose a secret affecting him.” *People v. Bollaert*, 248 Cal. App. 4th 699, 725 (2016) (citing Cal. Penal Code §519 and *Flatley v. Mauro*, 139 P.3d 2, 19 (Cal. 2006)). A “threat may be implied from all of the circumstances” and can be made using innuendo, including an innuendo in which “victims could infer that if they did not pay, the offensive content would remain on the site in further public view.” *Id.* at 725–26. The lack of “affirmative action to seek out or contact the victims but merely [to respond] to the victims’ pleas to remove their content, does not render the threat element unsupported by the evidence.” *Id.* at 726.

Additionally, Cal Penal Code § 523 provides that “[e]very person who, with intent to extort property or other consideration from another, sends or delivers to any person any letter or other writing, whether subscribed or not, expressing or implying, or adapted to imply, any threat such as is specified in Section 519 is punishable in the same manner as if such property or other consideration were actually obtained by means of such threat.” *Id.*

Reflex has specifically alleged that Web Presence solicits payments from victims and remits part of that payment, often (or entirely) through cryptocurrency, to the Extortion Websites to remove humiliating and defamatory accusations, including, for example, that the victim is a predator that “offer[s]

sex for money and [is] associated with child predation” by having one’s identifying information and picture posted on a webpage next to a “video depicting an adult male preying on a female child.” (*See* SAC at ¶ 3 & n. 4.) Failure to pay for removal will result in the continued display of the extortive identifying information. (*Id.* at ¶ 3.) Web Presence itself refers to these types of posts as slander, blackmail, and defamation—which shows that Web Presence is well aware of the illegality of the content that it charges to remove. (*See Id.* at ¶ 74.) This more than alleges extortion.

In addition to its allegations, the SAC provides the image of an actual email from Web Presence regarding a removal request from PredatorsAlerts.com to a SA Member which states, in part: “*We have 100% success rate with this site and removal takes about 72 hours and is guaranteed for life. The cost of removal is \$950.00.*” (*See* SAC at ¶ 70; *see also* SAC at ¶ 71, showing payment for removal of a post from PredatorsAlerts.com) (emphasis added).⁵ Under the prevailing law, this cannot be read other than as a threat to the SA Member to either pay \$950.00 to Web Presence for removal services or face continued exposure of either “deformity, disgrace or crime,” or a “secret” within the meaning of the California extortion statute.⁶ *See Bollaert*, 248 Cal. App. 4th at 725–26; *see* Cal. Penal Code §§ 518, 519 and 523. This—even setting aside Web Presence’s links with the Extortion Sites, Aaron Wallace (who, as alleged, is responsible for all but one of the Extortion Sites), Arman Ali (who, as alleged, is one of several data miners (“Data Miners”) responsible for harvesting Reflex’s customer information), and other Data Miners—is a more than adequate allegation (backed by an email) that Web Presence made wrongful extortion threats. (*See* SAC at ¶ 3).

(2) The Communication Decency Act Provides No Protection for Web Presence.

Even in the face of these allegations, Web Presence argues that its alleged conduct, standing alone, was legal. (*See* ECF No. 92 at 5:1-28, 6:16-18). To plead its innocence, Web Presence points to *Levitt v. Yelp! Inc.*, 765 F.3d 1123, 1129 (9th Cir. 2014) which it mischaracterizes as standing for the proposition that the Communications Decency Act of 1996 (“CDA”) immunizes Web Presence from extortion for charging fees for the removal of any content. (*See* ECF No. 92 at 5:15-19). However, *Levitt* expressly did not address the defense of immunity under the Communication Decency Act (CDA) in relation to extortion

⁵ Reflex notes that these allegations are sufficiently specific as to Web Presence’s conduct in furtherance of a civil conspiracy to extort as alleged in the SAC and discussed in Section IV(b).

⁶ Pleading fraud is not necessary for an extortion claim because the elements of extortion do not involve fraud. *See* Cal Penal Code §§ 518, 519 and 523

claims. *Levitt*, 765 F.3d at 1129 & 1137 n. 8 (“[W]e do not address Yelp’s defense of immunity under the CDA” and “[a]gain, we are not considering whether the CDA would pose a barrier to any such claims [of extortion]”); *also Bollaert*, 248 Cal. App. 4th at 730 (“*Levitt*’s holding did not turn on Yelp’s status as an interactive computer service or CDA immunity, which the Ninth Circuit expressly did not address”).

In fact, the *Bollaert* Court said that “we do not follow [*Levitt*] in any event” and doubted that *Levitt* was consistent with California law. *See id.* at 730. But most importantly, *Bollaert* limited the *Levitt* holding only to a recognition that legitimate economic threats as part of standard business practice are not extortion. *See id.* at 730. For example, “a mobilehome park operator does not commit extortion by telling tenants who refused to sign leases that they would have to pay their own utility bills.” *See id.* at 729. But—said the *Bollaert* Court—this is a far cry from a “threat...[of] continued exposure of private personal information resulting in a violation of the victims’ privacy rights and emotional distress.” *Id.* at 730. Such “conduct is nothing like the legitimate” tactics discussed in *Levitt*.” And, “unlike the plaintiffs in *Levitt*...the plaintiff victims here ***had a preexisting right—under privacy law—to be free of Bollaert’s threatened harm and not have their personal identifying information solicited and placed on UGotPosted.com without their consent.***” *Id.* (emphasis added). Thus, as per *Bollaert*, *Levitt* does not apply to extortion schemes (if it applies at all), and it certainly does not apply on the facts alleged here.

With or without Web Presence’s *Levitt* argument, the CDA provides no protection to the defendants here. The CDA does not protect the content on the Extortion Websites here because it is manufactured and/or solicited by the Extortion Websites, which, as alleged, Web Presence knows or should know (*see* SAC at ¶¶ 3 & n. 4, 7, 8, 74, 95, 97, 103), nor does it protect the communications, extortion threats, and requests for money to take down extortive content that Web Presence admits having done (Motion to Dismiss (ECF No. 92) at 2-3) and *for which Web Presence is directly liable*. *See Bollaert*, 248 at 721; 47 U.S.C. § 230 (f)(3).

The CDA only protects those who do not solicit or provide content, providing that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information ***provided by another information content provider.***” 47 U.S.C. § 230(c)(1) (emphasis added). An ‘information content provider’ is “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer

service.” 47 U.S.C. § 230(f)(3). “Information content providers” are *not* immunized by the CDA, and *Bollaert* has eliminated that defense for the Extortion Scheme participants. *See Bollaert*, 248 Cal. App. 4th at 710 (citing 47 U.S.C. § 230(f)(3)). This includes not just the visible extortive content on the Extortion Sites but also the related communications and extortive acts in which Web Presence admits it engaged, which are exactly the type that is excluded from CDA protection under *Bollaert*. *See Bollaert*, 248 Cal. App. 4th at 721 (citing *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1170 (9th Cir. 2008)).

For the visibly extortive content, websites that solicit unlawful content “materially contribute[s] to the illegality of the content and the privacy invasions suffered by the victims” are ‘information content providers’ that are excluded from CDA immunity. *Bollaert*, 248 Cal. App. 4th at 721 (citing *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1170 (9th Cir. 2008)). The Extortion Scheme participants here are “information content providers” outside of CDA immunity, because they collected victim information and posted that information alongside a defamatory accusation and a video about child predators (see SAC at ¶¶ 3, n. 4) (victims otherwise ended up on the Extortion Websites only because those Websites solicited their users to submit information on “predators.”) Because the Extortion Scheme participants created and/or solicited unlawful content for the purpose of extorting their victims, facts, as alleged, of which Web Presence was or should have been aware (see SAC at ¶¶ 3 & n. 4, 7, 8, 74, 95, 97, 103), those participants are ‘information content providers’ within the meaning of U.S.C. § 230(f)(3) and are not immunized from liability for the contents of those posts by the CDA. *See* 47 U.S.C. § 230(f)(3); *Bollaert*, 248 Cal. App. 4th at 710. Web Presence is liable for this conduct as a conspirator with knowledge of the relevant portions of the scheme as alleged in the SAC. (See SAC at ¶¶ 3 & n. 4, 7, 8, 74, 95, 97, 103).

For the related extortive communications, Web Presence itself is an “information content provider” as it authored the extortion threat email shown in paragraph 70 of the SAC *and* the website and press-release content to advertise removal (see ECF Nos. 84-8, 84-9, 84-10, SAC at ¶ 71). These communications “materially contribute to the illegality of the content” and are therefore not immunized from liability under the CDA. *See Bollaert*, 248 Cal. App. 4th at 721; 47 U.S.C. § 230(f)(3). Accordingly, neither Web Presence’s communications nor Web Presence is immunized by the CDA. *See id.*; *see also*

Gene Zorkin, “Sugar Dating” Site Sues Over Alleged Extortion of its Members, YNOT (Aug. 21, 2018), <https://www.ynot.com/sugar-dating-site-sues-extortion-members/> (last visited Nov. 15, 2018) (Observing that: “As described in Reflex’s complaint [ECF No. 1], the alleged scheme greatly resembles an approach employed by some revenge porn sites – and which ultimately led to the conviction of Kevin Bollaert”).

The defenses Web Presence raises here have already been rejected. In *Bollaert*, several individuals discovered that their identifying information—such as their names, hometowns and photos—had been posted to a revenge porn extortion website, UGotPosted.com, which was owned and operated by Kevin Bollaert. *Bollaert*, 248 Cal. App. 4th at 705–06. The extortion website “contained a link to [a reputation website], ChangeMyReputation.com, where victims were told that for payment of a specified amount of money, their pictures and information would be taken down.” *Id.* “According to Bollaert (*see* ECF No. 92 at: 6:15-19,)), (1) [Bollaert] was [‘]engaging in standard business practice,[’] and not extortion, similar to the practices approved by the Ninth Circuit in *Levitt v. Yelp! Inc.* (9th Cir.2014) 765 F.3d 1123 (*Levitt*),” and (2) “there is no evidence he directly or impliedly threatened any of the victims, and that the information, which was already publicly available and exposed on his [extortion website], cannot constitute a secret for purposes of extortion.” *Bollaert*, 248 Cal. App. 4th at 834.

The *Bollaert* Court roundly dismissed these arguments, holding that: (1) *Levitt* does not apply in cases where the threat is “continued exposure of private personal information resulting in a violation of the victims’ privacy rights and emotional distress” (*Id.* at 729–30); and (2) the threat of continued exposure of information posted online ***is sufficient to establish a threat and a secret within the meaning of the California extortion statute***, because the offending content remained a secret to persons who had not viewed it and its discovery would cause further humiliation or damage to the victims’ reputations. *Id.* at 728. As the *Bollaert* Court concluded:

[T]he threats were inherent and implied in the very structure and content of Bollaert's [extortion and reputation websites] which Bollaert himself created and operated. When victims were directed via [the extortion website] to the [reputation website], they were informed either via the [reputation website] or e-mail they could have their photos removed for a fee, from which victims could infer that if they did not pay, the offensive content would remain on the site in further public view. Those victims who communicated with [the reputation website] before they paid were told the content would only be removed upon payment, and [the reputation website] only removed the content when the victims paid the requested fee, which eventually was deposited in Bollaert's personal account. There is no question based on the victims' testimony that the display of their private images and information subjected them to shame, disgrace and embarrassment as to their reputation and character, and they would continue to be exposed to

other people if the content was not removed. The fact Bollaert did not take affirmative action to seek out or contact the victims, but merely responded to the victims' pleas to remove their content, does not render the threat element unsupported by the evidence [...] Bollaert's act in removing the victims' personal identifying information from [the extortion website], which he expressly solicited in the first place, did not give him a lawful right to collect a fee.

Id. at 726 (emphasis added).

The Extortion Scheme complained of in the SAC is a carbon copy of the scheme in *Bollaert*, merely involving a larger number of participants to carry out the scheme's objectives. As alleged, the outsourcing of some of the schemes' activities to co-conspirators is as follows: (1) Aaron Wallace outsourced communication with victims and collection of payments to Web Presence and the other Reputation Websites (compare SAC at ¶¶ 3, 50-71 with *Bollaert*, 248 Cal. App. 4th at 699), and (2) the Data Miners (as that term is defined in the SAC at ¶ 9) to illegally harvest information (and victims) from SeekingArrangement.com to upload to the Extortion Websites (see SAC at ¶¶ 3, 9, 16, 40-47). This multi-party conduct does not change the nature of the conduct or the scheme or in any way legitimize it; to the contrary, these differences make more parties, including Web Presence, responsible for all actions performed in furtherance of the Extortion Scheme.

(b) WEB PRESENCE IS A KNOWING AND WILLING PARTICIPANT IN THE EXTORTION SCHEME CONSPIRACY.

The Extortion Scheme involves a civil conspiracy, which is the "combination of two or more persons who, by some concerted action, intend to accomplish some unlawful objective for the purpose of harming another which results in damage." *Gilbrook v. City of Westminster*, 177 F.3d 839, 856 (9th Cir. 1999), *as amended on denial of reh'g* (July 15, 1999) (quoting *Vieux v. East Bay Reg'l Park Dist.*, 906 F.2d 1330, 1343 (9th Cir.1990)). "To prove a civil conspiracy, the plaintiff must show that the conspiring parties reached a unity of purpose or common design and understanding, or a meeting of the minds in an unlawful agreement." *Id.* **Error! Bookmark not defined.** "To be liable, each participant in the conspiracy need not know the exact details of the plan, but each participant must at least share the common objective of the conspiracy." *Id.* "A defendant's knowledge of and participation in a conspiracy may be inferred from circumstantial evidence and from evidence of the defendant's actions." *Id.* (emphasis added). "Tacit consent as well as express approval will suffice to hold a person liable as a coconspirator." *Wyatt v. Union Mortg. Co.*, 598 P.2d 45, 52 (1979). "[I]t is not necessary that [a conspiracy participant] should have joined the conspiracy at the time of its inception; every one who enters into such a common design is in

law a party to every act previously or subsequently done by any of the others in pursuance of it.” *de Vries v. Brumback*, 349 P.2d 532, 535 (1960).⁷

Here, Reflex has in fact alleged a conspiracy by Defendants who worked together with the ultimate goal of extorting money from their victims, including SA Members, by way of humiliating and defamatory postings. (SAC at ¶¶ 1, 3, 22-23, 48-71, 82, 90, 95, 103 100, 110, 117). And allegations supported by correspondence from Minc, LLC (also referred to in the complaint as “DRL”) show that SA Members requesting removal from one of the removal outlets, such as Web Presence, stated that they were members of SeekingArrangement.com: “We have seen a lot of clients tell me they signed up for seeking arrangements. We don’t know what the connection is between online dating and this site but this is something I have seen and heard over the past 4 months.” (SAC at ¶¶ 95, 103). Accordingly, allegations that Web Presence’s knowledge that the extortion victims were often Reflex’s customers is not merely speculative; it is supported by actual reports made by victims to payment processors doing the same thing that Web Presence admits in its Motion (Motion to Dismiss (ECF No. 92) at 2) that it did when it took victims’ money. (*See id.*)

Here are just a few specific examples of the conspiracy alleged in the SAC:

(1) A tacit agreement: “Based on these guarantees, quick turnaround times [including lifetime removal guarantees, 100% removal success, a 72 hour removal estimate and actual 20 minute removal by Web Presence], and the facts below regarding the representations made by the various internet content removal service providers (including the Removal Sites) and the collection of email provided by the owner of a fellow removal provider, DRL [showing the process by which removal from Aaron Wallace’s extortion websites occurs], Plaintiff Reflex Media believes that the Extortion Websites and the Removal Sites have an agreement that allows the Removal Sites to remove content from the Extortion Websites in exchange for payment, with the understanding that the Extortion Websites will generate clients for the Removal Sites.” (SAC at ¶ 56); *see also* Web Presence’s Motion to Dismiss, ECF No. 92 at 2:16-18 (“When the removal of negative content is a viable option, Web Presence will contact the website where that content is hosted to determine whether it will voluntarily remove that material. If a host site is willing

⁷ Civil conspiracy does not involve fraud and is not subject to Rule 9(b)’s heightened pleading standards. *Compare* Hanger Prosthetics & Orthotics, Inc., 556 F. Supp. 2d at 1131 (“defraud” may be used to mean “wrongdoing” and does not require proof of common law fraud”) with Cal. Penal Code §§518, 519 & 523 (showing an absence of the elements of fraud).

1 to remove the content, it typically charges a fee for that service.”)

2 (2) A wrongful act done pursuant thereto: Web Presence sent an email amounting to an
3 extortion threat and was paid money to remove humiliating information from PredatorsAlerts.com (and
4 consequently must have paid Aaron Wallace to remove information from his website,
5 PredatorsAlerts.com). (See SAC at ¶¶ 3, 7, 70–71; see discussion in Section IV(a)(1)).

6 (3) Damage resulting from such act or acts: a) “Defendants’ illegal operation has caused harm
7 to Reflex Media through the loss of SA Members and through damage to Reflex Media’s reputation and
8 brand as a safe and discreet place for people to find relationships on their terms.” (SAC at ¶ 4). b) A “SA
9 Member has stated that the Member had a big problem with PredatorAlerts.com, did not feel safe, and
10 would end his or her membership with SeekingArrangement.com as a result.” (SAC at ¶ 21).⁸

11 As alleged, Web Presence knew that it was part of an unlawful extortion scheme and that it was
12 harming SeekingArrangement.com, and thereby Reflex, by its actions. Web Presence’s actions were
13 illegal and part of an unlawful and tacit (at the least) extortion agreement with the Extortion Sites.⁹
14 Therefore, Reflex has successfully alleged a conspiracy between Web Presence and the other Defendants.
15 And Web Presence’s purported “factual” defenses (if any) are irrelevant at this 12(b)(6) stage of the case,
16 as Reflex has more than plausibly alleged that Web Presence is a willful and knowing party to a conspiracy
17 that harmed Reflex and therefore responsible for all tortious actions by the participants in furtherance of
18 the conspiracy, including, intentional and negligent interference with prospective economic advantage,
19 CFAA violations, Cal. Penal Code § 502 violations, and unfair competition. *See de Vries*, 349 P.2d at 535.

20 (c) **THE SECOND AMENDED COMPLAINT IS SUFFICIENTLY CLEAR AS TO THE ROLES OF**
21 **EACH EXTORTION SCHEME PARTICIPANT.**

22 The SAC is sufficiently clear as to the roles of each member of the Extortion Scheme. While this

23 ⁸ Reflex also notes that on page 4:20–22, Web Presence makes incorrect and irrelevant assertions that
24 “Plaintiff’s SAC fails to allege any specific connection, agreement, or plan between Defendant Arman Ali
25 and other Doe Defendants (collectively, as referred to in Plaintiff’s SAC, the “Data Miner Defendants” or
26 “Data Miners”). (See SAC at ¶ 9 (“Arman Ali [] does business under the fictitious name D4 Solutions BD
27 [...] D4 Solutions, through **Ali himself**, or his employees and/or agents, act as data miners (sometimes
28 referred to as Data Miners) by creating fake profiles on SeekingArrangement.com for the purpose of
creating decoy accounts that he uses to collect other users’ names, phone numbers, locations and photos
and then uses or sells that information to the Extortion Websites.” (internal quotation marks omitted,
emphasis added).)

⁹ As alleged, Wallace and Web Presence’s actions cannot be “unchoreographed” because each took actions
in direct response to the actions of the other – *i.e.* Wallace removed a posting from PredatorsAlerts.com
because Web Presence was able to extort a SA member and remitted payment to him. (See SAC at ¶¶ 3d,
71).

is more elaborately discussed in Section IV (b) above, Web Presence admits to this very fact by stating: “Plaintiff references multiple or all Defendants, and **alleges that they are all doing completely different actions.**” (ECF No. 92 at 20:22–23) (emphasis added). Because Reflex’s allegations are clear as to what actions that Web Presence took in furtherance of the Extortion Scheme, it cannot complain that it does not know what is alleged against it. Moreover, Web Presence’s and the other defendants’ specific acts are described in detail throughout the SAC as discussed in further detail herein, Sections IV (a–b, d–g), and the SAC, itself. (*See generally*, SAC.)

(d) EXTORTION SCHEME PARTICIPANTS VIOLATED THE COMPUTER FRAUD AND ABUSE ACT, GIVING THIS COURT SUBJECT MATTER JURISDICTION, AND CALIFORNIA PENAL CODE §502.

It is settled law that the Computer Fraud and Abuse Act and California Penal Code section 502 covers unauthorized access of a computer system (not merely “hacking”). Hence, Web Presence’s argument that such unauthorized access is merely a breach of contract contradicts both the statutes and the case law. (And of course, the same conduct can be *both* a breach of contract as well as a CFAA violation and a predicate for other causes of action).

(1) Reflex Has Made Numerous and Detailed Allegations Relating to Computer Crimes, Including the Following

1. “[A]t the direction of Aaron Wallace, at least some Defendants referred to herein as Data Miners are creating fake profiles on SeekingArrangement.com (the “Decoy Profiles”) that they use to meet and communicate with SA Members for the purpose of collecting their names, phone numbers, locations, and photos so that they and/or other Defendants can post that information on the Extortion Websites.” (SAC at ¶ 40 (emphasis in the original)).¹⁰

2. “The Decoy Profiles have been shut down by Reflex Media as they have been identified and the Data Miners have been permanently banned from using SeekingArrangement.com for any purpose.” (SAC at ¶ 43).

3. “Wallace’s scheme involved circumventing barriers to mining information. Reflex sent emails to the Data Miners at various addresses that the Data Miners provided to create their Decoy

¹⁰ As Web Presence’s Motion stands or falls based on the sufficiency of Reflex’s allegations in the SAC, Web Presence’s references to what was said in “Plaintiff’s Reply in Support of Motion for Additional Time to Conduct Discovery to Identify Doe Defendants (Dkt. 82), and at oral argument held on February 19, 2019” are irrelevant. *See* ECF No. 92 at 4. *Butler v. Los Angeles Cty.*, 617 F. Supp. 2d 994, 999 (C.D. Cal. 2008) (“the Court must limit its review to the four corners of the operative complaint”).

1 Profiles. The emails told the Data Miners that Reflex had permanently banned the Data Miners from use
 2 of SeekingArrangement.com and all other Reflex owned websites for any purpose. Furthermore, Reflex
 3 set up internet protocol address blocks against several internet protocol addresses that it believes the
 4 Data Miners used to effectuate their illegal scheme.” (SAC at ¶ 44).

5 4. “Nevertheless, the Data Miners continue to return to SeekingArrangement.com and **gain,**
 6 or attempt to gain, **unauthorized access to the website using fake email accounts and virtual private**
 7 **network technology.** This “whack-a-mole” pattern continues today and **detracts valuable resources**
 8 **from Reflex Media’s regular operations** to prevent their illegal actions” (SAC at ¶ 45, emphasis
 9 added).

10 5. “Defendants’ conduct has caused loss, as defined in 18 U.S.C. § 1030(e)(11) of more than
 11 \$5,000 to Reflex Media during a one-year period.” (SAC at ¶ 83).

12 6. “Defendants referred to herein as Data Miners are [...] collecting [SA Members] names,
 13 phone numbers, locations, and photos so that they and/or other Defendants can post that information on
 14 the Extortion Websites.” (SAC at 40).

15 7. “[F]or every 100 personal profiles mined from SeekingArrangement.com, [D4 Solutions,
 16 aka Arman Ali’s] agents will be paid 200 Bangladeshi taka.” (SAC at ¶¶ 41, 47).

17 8. A “SA Member reported [...] paying a \$699 removal fee to Web Presence” (SAC at ¶ 71).

18 **(2) Defendants’ Unlawful Access Gives Rise to a Sufficiently Pled and Valid**
 19 **CFAA Claim.**

20 Web Presence’s argument with respect to the federal Computer Fraud and Abuse Act (“CFAA”),
 21 fails on the law. Web Presence maintains that the CFAA only covers “hacking” and simply doesn’t apply
 22 to unauthorized system access (as is alleged here). (*See* ECF No. 92 at pp. 14–15). This contention fails,
 23 as—to begin with—the CFAA says nothing about “hacking.” In fact, the courts in the Ninth Circuit have
 24 rejected this identical argument. *See e.g., Ticketmaster L.L.C. v. Prestige Entm’t W., Inc.*, 315 F. Supp. 3d
 25 1147, 1169 (C.D. Cal. 2018) (finding “successful pleading of a CFAA violation doesn’t depend on whether
 26 any Defendant hacked anything”).

27 The *Ticketmaster* Court held that the CFAA “provides two ways of committing the crime of
 28 improperly accessing a protected computer: (1) obtaining access without authorization; and (2) obtaining
 access with authorization but then using that access improperly.” *Ticketmaster*, 315 F. Supp. 3d at 1169

(citing *Musacchio v. United States*, 136 S.Ct. 709, 713, 193 L.Ed.2d 639 (2016)). The *Ticketmaster* Court also held that where a defendants’ “business model is built on a scheme to evade [Plaintiff’s] policies for profit,” that simply sending “an individualized Letter to [d]efendants instructing them to cease their activities” is enough to revoke authorization under the CFAA, and technical barriers do not need to be put in place. *Id.* at 1170.

In so holding, the *Ticketmaster* Court was following additional established and relevant Ninth Circuit precedent. See *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016) (hereinafter, “*Power Ventures*”) (“[A] defendant can run afoul of the CFAA when [the defendant’s] permission [to access] has been revoked explicitly. Once permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability.”). Further, a defendant’s actions to circumvent technological barriers, such as an IP block, demonstrate that the plaintiff has revoked access to that defendant, and that the defendant is aware of that revocation (although such actions are not required to state either a CFAA or Cal. Penal Code § 502 claim). See *Power Ventures*, 844 F.3d at 1068–69. Furthermore, *Power Ventures* held that the same sort of activity alleged in the SAC—obtaining access without authorization to disseminate messages on Facebook’s website and to collect information from Facebook users—was a CFAA violation. *Id.* at 1065–68; see *Ticketmaster L.L.C.*, 315 F. Supp. 3d at 1168 (holding that when a plaintiff alleges that a defendant (1) accesses protected computers without authorization and (2) that access caused Plaintiff an aggregate ‘loss’ of \$5,000 in any one-year period, “it need only further plead that Defendants obtained [‘]information,[’]” thereby violating the CFAA); see also 18 U.S.C. § 1030 (a)(7)(B-C) (providing additional bases for liability under the CFAA).

Reflex’s allegations here meet this standard. Reflex has specifically alleged that collection of Reflex’s user information for the Extortion Websites exceeded the terms of permitted access *and* that the collectors persisted even after being specifically banned by Reflex and having their IP addresses blocked. As stated in the SAC: “Reflex sent emails to the Data Miners at various addresses that the Data Miners provided to create their Decoy Profiles. The emails told the Data Miners that Reflex had permanently banned the Data Miners from use of SeekingArrangement.com and all other Reflex owned websites for any purpose. Furthermore, Reflex set up internet protocol address blocks against several internet protocol addresses that it believes the Data Miners used to effectuate their illegal scheme.” (SAC at ¶ 44, emphasis

added). “Nevertheless, the Data Miners continue to return to SeekingArrangement.com and **gain**, or attempt to gain, **unauthorized access to the website using fake email accounts and virtual private network technology**. This “whack-a-mole” pattern continues today and **detracts valuable resources from Reflex Media’s regular operations** to prevent their illegal actions.” (SAC at ¶ 45, emphasis added). “Defendants’ conduct has caused loss, as defined in 18 U.S.C. § 1030(e)(11) of more than \$5,000 to Reflex Media during a one-year period.” (SAC at ¶ 83). Detracting valuable resources from Reflex’s regular operations to identify the offending accounts and constitutes loss under the CFAA. *See SuccessFactors, Inc. v. Softscape, Inc.*, 544 F. Supp. 2d 975, 981 (N.D. Cal. 2008) (finding that “discovering who has that information and what information he or she has is essential to remedying the harm”). Reflex also alleged that Defendants collected information: “Defendants referred to herein as Data Miners are [...] collecting [SA Members] names, phone numbers, locations, and photos so that they and/or other Defendants can post that information on the Extortion Websites.” (SAC at 40). And that information is ‘anything of value’: “for every 100 personal profiles mined from SeekingArrangement.com, [D4 Solutions, aka Arman Ali’s] agents will be paid 200 Bangladeshi taka,” (SAC at ¶¶ 41, 47); and a “SA Member reported [...] paying a \$699 removal fee to Web Presence” (SAC at ¶71).

Thus, Reflex has more than sufficiently pled a claim under the CFAA. Reflex has specifically alleged improper use of access by the Data Miners, and persistence in improper use after being informed that they no longer have access. This constitutes a valid CFAA cause of action under the Ninth Circuit and district court precedent stated, and under that precedent Web Presence’s, “[T]his is just a breach of contract,” argument must fail. And because Reflex has pled a claim under the Computer Fraud and Abuse Act, which is a federal statute, this Court has subject matter jurisdiction (including supplemental jurisdiction) over this action. *See* 18 USC § 1030 *et seq.*; *see* 28 U.S.C. § 1331; *see* 28 U.S.C. § 1367 (“[T]he district courts shall have supplemental jurisdiction over all other claims that are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy”).

(3) Defendants’ Unpermitted Access is Sufficiently Pleaded to State a Valid Cause of Action Under California Penal Code § 502.

The same result applies for Reflex’s claim under California Penal Code § 502 (Count I). This law is similar to the CFAA, but only requires that a defendant has “knowing access without permission.” *See* subparagraphs of Cal. Penal Code § 502(c); *Power Ventures*, 844 F.3d at 1069 (citing *United States v.*

1 *Christensen*, 801 F.3d 970, 994 (2015)); *see In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1099 (N.D. Cal.
 2 2015) (“Nothing in the *Power Ventures* decision held that overcoming [“]technical or code-based
 3 barriers[”] designed to prevent access was the only way to establish that the Defendant acted without
 4 permission”). If a defendant accesses a computer, as that term is defined in Cal. Penal Code § 502, that
 5 they know they do not have permission to access, he or she is in violation of the code. *See* Cal. Penal Code
 6 § 502; *see Power Ventures*, 844 F.3d at 1069.

7 **(e) REFLEX SUCCESSFULLY PLED INTENTIONAL AND NEGLIGENT INTERFERENCE WITH**
 8 **PROSPECTIVE ECONOMIC ADVANTAGE, AND UNFAIR COMPETITION CAUSES OF ACTION**

9 Web Presence does not challenge Reflex’s intentional and negligent interference with prospective
 10 economic advantage claims other than on the basis that it purports not to have engage in extortion. (Motion
 11 to Dismiss (ECF No. 92) at 21:18-22.) For the reasons set out in detail in Section IV (a) above, Web
 12 Presence’s cursory argument on this point fails. As to the elements of the interference causes of action,
 13 Reflex sufficiently pleaded these as well. (*See* SAC at ¶¶ 93–110 and SAC *generally* (pleading the
 14 requisite economic relationship, knowledge of that relationship, intentional and negligent acts, disruption
 15 of the relationship and economic harm)); *see also Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal.
 16 4th 1134, 1153, 63 P.3d 937, 950 (2003) (detailing the elements of intentional interference with
 17 prospective economic advantage) and *N. Am. Chem. Co. v. Superior Court*, 59 Cal. App. 4th 764, 786, 69
 18 Cal. Rptr. 2d 466 (1997) (detailing the elements of negligent interference with prospective economic
 19 advantage). To successfully allege a statutory unfair competition claim under Cal. Bus. & Prof. Code §
 20 17200 (the “UCL”), Reflex need not allege a specific subsection under “Chapter 1 (commencing with
 21 Section 17500) of Part 3 of Division 7 of the Business and Professions Code,” but only a violation of some
 22 other law. The UCL establishes “three varieties of unfair competition.” *Cel-Tech Commc’ns, Inc. v. L.A.*
 23 *Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999). The first variety prohibits any unlawful business practice
 24 as defined by other sources of federal and California law, for which the UCL “borrows violations of other
 25 laws and treats them as unlawful practices that the unfair competition law makes independently
 26 actionable.” *Id.* “Violations of other laws” include extortion, CFAA, California Penal Code §502
 27 violations, and intentional and negligent interference. *See Saunders v. Superior Court*, 27 Cal. App. 4th
 28 832, 837–39, (1994); *compare Levitt*, 765 F.3d at 1129–30 with *Bollaert*, 248 Cal. App. 4th at 725–30.

Nor are Reflex’s statutory and common law unfair competition claims duplicative. *See BriteSmile*,

1 *Inc. v. Discus Dental, Inc.*, No. C 02-03220 JSW, 2005 WL 3096275, at *6 (N.D. Cal. Nov. 18, 2005)
 2 (citing *Duncan v. Stuetzle*, 76 F.3d 1480, 1489 (9th Cir.1996) and *Smith & Hawken, Ltd. v. Gardendance*,
 3 *Inc.*, 2004 WL 2496163, *10, 2004 Copr. L. Dec. P 28,903, RICO Bus. Disp. Guide 10,787 (N.D. Cal.
 4 Nov.5, 2004)) (holding that unfair competition claims under the UCL and common law are not duplicative
 5 because (1) these causes of action provide a theoretical state law basis for a plaintiff's requested relief, (2)
 6 the claims are not identical, and (3) and punitive damages are available under common law but not under
 7 the UCL).

8 For the above reasons, Reflex has adequately alleged its Counts III through VI.

9 **(f) REFLEX DOES NOT RELY UPON FRAUD TO STATE ITS CAUSES OF ACTION**

10 Web Presence tries to impose Rule 9(b)'s heightened pleading standards (for fraud) on all of
 11 Plaintiff's claims by way of the summary assertion that "[a]ll of Plaintiff's claims, insofar as they relate
 12 to Web Presence, allege that Web Presence engaged in a conspiracy to defraud members of Plaintiff's
 13 website, SeekingArrangement.com." (ECF No. 92 at 7). Web Presence makes this broad statement that
 14 the entire case against them is based in fraud without citing to a single claim for fraud, a single element
 15 of a claim requiring fraud much less reliance thereon, or even an allegation of fraud. Reflex's SAC
 16 contains substantial, detailed allegations supporting its claims and surely could survive the application of
 17 this standard, however it doesn't have to because the standard is inapplicable here.

18 Reflex hasn't brought a claim for fraud, and Web Presence cannot credibly argue that the entire
 19 SAC 'sounds in fraud' for purposes of Rule 9(b). Reflex has raised a claim under Computer Fraud and
 20 Abuse Act ("CFAA") but there is no need to plead the elements of fraud or comply with 9(b) to make
 21 out a claim under the CFAA. *See NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 833 (N.D.
 22 Cal. 2014) ("Violations of subsections (a)(2) and (a)(5) [of the CFAA] do not need to be pled with
 23 particularity" ... "most CFAA cases in this district have not applied Rule 9(b)'s pleading standards to all
 24 CFAA claims") (quoting *Prop. Rights Law Grp., P.C. v. Lynch*, No. 13-00273, 2013 WL 4791485, at *4
 25 (D.Haw. Sep. 16, 2013); *eBay Inc. v. Digital Point Sols., Inc.*, 608 F. Supp. 2d 1156, 1164 (N.D. Cal.
 26 2009) (finding that "the CFAA only requires a showing of unlawful access; there is no need to plead the
 27 elements of common law fraud to state a claim under the Act")); *Facebook, Inc. v. MaxBounty, Inc.*, 274
 28 F.R.D. 279, 284 (N.D.Cal.2011) (citing *eBay* ; "The Court sees no reason to depart from its previous

analysis.”); *Multiven v. Cisco*, 725 F.Supp.2d 887, 892 (N.D.Cal.2010) (“For purposes of the CFAA, [t]he term “defraud” ... simply means wrongdoing and does not require proof of common law fraud.”) (citation omitted). Moreover, the use of the term “defraud” does not magically elevate a CFAA cause of action into a Rule 9(b)-governed fraud claim. *See Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc.*, 556 F. Supp. 2d 1122, 1131 (E.D. Cal. 2008) (stating that “for purposes of § 1030(a)(4) [of the CFAA, the term ‘defraud’] simply means wrongdoing and does not require proof of common law fraud.”)

Even if the underlying activity directed at Reflex’s users involved actual fraud, pleading a CFAA claim does not require heightened pleading where Reflex did not rely on the misrepresentation as a basis of any of its claims. *See Oracle Am.*, No. 5:13-CV-03385-PSG, 2014 WL 31344, at *5 (N.D. Cal. Jan. 3, 2014) (finding that Rule 9(b) pleading standards do not apply to CFAA allegations where a plaintiff does not rely on a misrepresentation by a defendant, even if its customers did). For the same reason, allegations concerning misstatements do not convert any or all other causes of action to fraud where those misstatements and reliance on those misstatements is not necessary to make out a claim. *See City & Cty. Of San Francisco.*, 957 F. Supp. at 1141; *Vess*, 317 F.3d at 1102–06; *Mirkin v. Wasserman*, 858 P.2d 568, 570 (1993). If that were true, every breach of contract involving a lie would have to be pleaded under 9(b), but that’s clearly not the case. *See id.* Hence, not a single claim or element of any claim in this case requires a misstatement much less reliance thereon in order to be properly pleaded. (*See SAC, Generally.*) Accordingly, the Rule 9(b) pleading standard does not apply to all or even any of Reflex’s claims.

(g) REFLEX’S DETAILED PLEADINGS EASILY SATISFY THE PLEADING STANDARD SET FORTH IN *TWOMBLY*.

The detailed allegations in the SAC and described in Sections IV (a–e) above easily satisfy the pleading standard set out in *Bell Atl. Corp. v. Twombly*. The applicable pleading standard set forth in *Twombly* and its progeny is that, when considering allegations in the complaint, the “court does not require heightened fact pleading of specifics;” it only requires “enough facts to state a claim to relief that is plausible on its face.” *World Health & Educ. Found.*, 612 F. Supp. at 1093 (N.D. Cal. 2009) (citing *Twombly*, 550 U.S. at 570) (internal quotations omitted). The court should consider the entire factual conduct alleged in a complaint to analyze whether a plaintiff has “[nudged its claim] across the line from conceivable to plausible.” *See Soo Park*, 851 F.3d at 928 “The *Twombly* plausibility standard ... does not

1 prevent a plaintiff from pleading facts alleged upon information and belief where the facts are peculiarly
 2 within the possession and control of the defendant or where the belief is based on factual information that
 3 makes the inference of culpability plausible.” *Id.*; *see also Concha v. London*, 62 F.3d 1493, 1503 (9th
 4 Cir. 1995) (“[W]e relax pleading requirements where the relevant facts are known only to the defendant.”).

5 Though set out in further detail in the SAC, in sum the allegations are that Web Presence directly
 6 and as a co-conspirator engaged in extortion and related conduct, giving rise to Reflex’s claims, as follows:

7 1. Web Presence knew or had reason to know that victims’ information was being solicited,
 8 harvested and posted to the Extortion Websites; (*see* SAC at ¶¶ 56, 95, 103).

9 2. Web Presence directly interfaced with people they knew to be extortion victims; (*see* SAC
 10 at ¶¶ 3, 70-72, 74, 82, 90, 100, 110, 117, 122)

11 3. Web Presence determined the amount to charge for removal; (*see* SAC at ¶¶ 3, 72)

12 4. Web Presence made offers to have their Extortion Website counterparts remove the
 13 information in exchange for the money and/or equivalent cryptocurrency; (*see* SAC at ¶¶ 3, 23, 71)

14 5. Web Presence took the victims’ money under the implicit threat that the extortive
 15 information would remain online if the victims didn’t pay; (*see* SAC at ¶¶ 3, 70, 71)

16 6. Web Presence shared that extortion profit with the Extortion Sites; (*see* SAC at ¶¶ 3, 23
 17 56, 70, 71)

18 7. Web Presence disguised and anonymized the extortion profit for the Extortion Sites by
 19 providing their portion of the funds in Bitcoin. *See* SAC at ¶ 3.

20 These allegations more than meet the plausibility standard for liability here because they set out
 21 the conduct establishing the elements of Reflex’s claims (as detailed further in Sections IV (a–e)) and
 22 demonstrates the existence of a conspiracy between the parties (as detailed further in Section IV (b)). *See*
 23 *Soo Park*, 851 F.3d at 928.

24 Moreover, the facts of a conspiracy in the SAC are not remotely like those in *Twombly* as Web
 25 Presence has incorrectly argued. *See e.g.* ECF No. 92 at 10:8–11 (citing *Twombly*, 550 U.S. at 565–66).
 26 *Twombly* was an antitrust case in which the plaintiff alleged parallel business conduct—market conduct
 27 among competitors that mimicked or tracked one another—to support a theory of conspiracy involving
 28 the defendants. *Twombly*, 550 U.S. at 546. In that case the court held “lawful parallel [unchoreographed]

conduct fails to bespeak unlawful agreement and is not enough to suggest a conspiracy.” *Id.* at 556.

Unlike in *Twombly*, Reflex does not allege any parallel business conduct to demonstrate the existence of a conspiracy. (See SAC at ¶¶ 3, 23, 26, 27, 56, 71). To the contrary, Reflex alleges choreographed conduct between the Extortion Websites (including Aaron Wallace’s websites) and Web Presence as each took actions in direct response to the actions of the other pursuant to specific terms that could only exist in the presence of an agreement between the parties—*e.g.*, an extortion victim’s information is posted, Web Presence takes the victim’s money and sends some of it to the Extortion Sites who then remove the extortive information from the extortion site on which it was posted. (See SAC at ¶¶ 3, 23, 26, 27, 56, 71). This is concerted conduct where one party acts and the other acts directly in response, exchanging information and money with one another and acting in direct response to one another’s requests to act pursuant to the terms of their agreements to do these exact things. (*Id.*) And Web Presence’s role and acts in actually engaging in extortion in furtherance of the Extortion Scheme is, itself, unlawful conduct. Thus, this isn’t anything like competitors acting similarly where one another’s conduct is publicly visible to be mimicked as was found insufficient under *Twombly*.

The *Twombly* opinion itself held “that stating such a claim requires a complaint with enough factual matter (taken as true) to suggest that an agreement was made. Asking for plausible grounds to infer an agreement does not impose a probability requirement at the pleading stage; it simply calls for enough facts to raise a reasonable expectation that discovery will reveal evidence of illegal agreement.” *Twombly*, 550 U.S. at 556. As already pointed out, “Tacit consent as well as express approval will suffice to hold a person liable as a coconspirator.” *Wyatt*, 598 P.2d at 52.

Web Presence made express representations to the extortion victims that “***“We have 100% success rate with this site and removal takes about 72 hours and is guaranteed for life. The cost of removal is \$950.00.”*** (See SAC at ¶ 70.) Rather than merely unchoreographed conduct of *Twombly*, Web Presence’s own statement demonstrates the presence of an agreement with at least these terms: (1) Web Presence had already been provided a removal fee price which allows it to create a markup, (2) Web Presence had a relationship with the Extortion Websites that allow it to “Guarantee” removal, and (3) PredatorsAlerts.com (Aaron Wallace) had given Web Presence assurances that the removal of extortive information from PredatorsAlerts.com is guaranteed for life.

On these bases, the pleading standards set forth in *Twombly* is met in the SAC.

(h) REFLEX MAY BRING CLAIMS BASED ON THE LAW OF OTHER FORUMS.

Curiously, Web Presence argues that Reflex cannot bring California claims because “Plaintiff does not have standing to bring California state law claims because it is not a California resident, and did not suffer the harms it complains about.” (ECF No. 92 at 91:27-28; 20: 1-9). But there is no legal principle stating that only California residents have standing to bring California claims, and the case law Web Presence cites relates to personal jurisdiction, not standing. (*Id.*) Here, however, personal jurisdiction exists because Web Presence is a Nevada Corporation so this Court has general jurisdiction and therefore “may hear any claim against that defendant, even if all the incidents underlying the claim occurred in a different State.” *Bristol-Myers Squibb Co. v. Superior Court of California, San Francisco Cty.*, 137 S. Ct. 1773, 1780, 198 L. Ed. 2d 395 (2017)¹¹. Hence, Web Presence’s personal jurisdiction and standing arguments do not apply.

And Reflex further alleges that the Extortion Scheme was country-wide, with acts directed at Reflex’s California customers that caused them to end their relationship with Reflex and caused damage to Reflex’s reputation in those states that it targeted. (*See* SAC at ¶ 1, 3, 4, 15, 16, 18, 22, 70, 71, 86).¹² It is also settled law that out-of-state plaintiffs may bring claims under the laws of other states—for instance, the U.S. Supreme Court in *Keeton v. Hustler Magazine, Inc.* found that a New York resident could bring a claim under the laws of New Hampshire for a nationwide suit. 465 U.S. 770, 778, 104 S. Ct. 1473, 1480, 79 L. Ed. 2d 790 (1984) (“[A]pplying New Hampshire’s statute of limitations to all aspects of this nationwide suit has nothing to do with the jurisdiction of the Court to adjudicate the claims”). Further still and finally, this case was transferred to Nevada pursuant to 28 U.S.C. § 1404(a), and under that statute, “when a suit is transferred pursuant to 28 U.S.C. § 1404(a), the substantive law of the state in which the suit was originally filed applies.” *Synthes, Inc. v. Knapp*, 250 F. Supp. 3d 644, 650 (E.D. Cal. 2017).

For of the above reasons, Reflex has ability to raise California law claims against Web Presence in this Court.

¹¹ Web Presence seems to confuse where actions took place and where harm is felt.

¹² For instance, Web Presence’s actions to extort SA Members make customers believe that there is a higher cost to be on SeekingArrangement.com because they may (or have had) to pay for removal services, and those same customers feel threatened for using SeekingArrangement.com.

(i) **THE NORTHERN DISTRICT OF CALIFORNIA HAS ALREADY FOUND THAT THIS COURT HAS SUBJECT MATTER JURISDICTION, PERSONAL JURISDICTION, AND IS A PROPER VENUE FOR THIS CASE**

Finally, Reflex points out that the law concerning transfers under 28 U.S.C. § 1404 provides that subject matter jurisdiction and venue have already been found by the court that transferred the case here. Web Presence already moved for dismissal on jurisdictional grounds before Judge Hamilton and lost (she transferred the case to the District of Nevada). (ECF No. 61.) And Judge Hamilton, in transferring the case here, cited to a prior judicial decision which said that: “An action [suitable for 28 U.S.C. § 1404(a) transfer] is one that might have been brought in the transferee court when (i) *the transferee court would have had subject matter jurisdiction at the time the action was filed*; (ii) *defendants would have been subject to personal jurisdiction*; and (iii) *venue would have been proper*.” *Thermolife Int’l, LLC v. Vital Pharm., Inc.*, No. CV142449RSWLAGRX, 2014 WL 12235190 at *2 (C.D. Cal. Aug. 15, 2014) (emphasis added) (cited in ECF No. 61 at 3:16); *E. & J. Gallo Winery v. F. & P. S.p.A.*, 899 F. Supp. 465, 466 (E.D. Cal. 1994) (same). In other words, Judge Hamilton, in transferring the case here, on the basis of the law cited, concluded that subject matter jurisdiction, personal jurisdiction, and venue were appropriate in the District of Nevada. For this reason as well, this Court has subject matter jurisdiction to hear this case.

V. CONCLUSION

For all the reasons stated above, Plaintiff Reflex Media, Inc., respectfully requests that Web Presence’s Motion to Dismiss be denied.

DATED: March 26, 2019

SMITH WASHBURN, LLP

/s/ Mark L. Smith
Mark L. Smith
Attorneys for Reflex Media, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on March 26, 2019, the foregoing **OPPOSITION TO WEB PRESENCE LLC'S MOTION TO DISMISS PLAINTIFF'S SECOND AMENDED COMPLAINT** was served on the person(s) named below via the Court's electronic filing system:

James D. Boyle, Esq.
Sean E Story, Esq.
400 South Fourth Street, Third Floor
Las Vegas, Nevada 89101
Email: jboyle@nevadafirm.com
sstory@nevadafirm.com

Chad T. Nitta
Becky Franson
Rachael Culhane
KUTAK ROCK LLP
1801 California Street, Suite 3000
Denver, CO 80202
Email: chad.nitta@kutakrock.com
becky.franson@kutakrock.com
rachael.culhane@kutakrock.com

Attorneys for Marca Global, LLC

Jean J. Schwartz
LAW OFFICES OF JEAN SCHWARTZ
10620 Southern Highlands Parkway, Suite 110-473
Las Vegas, Nevada 89141
Email: Jean.schwartz@gmail.com

Michelle L. Mozdzen
Christopher Ingle
MAY, POTENZA, BARAN & GILLESPIE, P.C.
Chase Tower, 201 N. Central Ave., 22nd Floor
Phoenix, AZ 85004
Email: mmozdzen@maypotenza.com
cingle@maypotenza.com

Attorneys for Web Presence, LLC

Michael Carrigan
SPIEGEL & UTRERA, P.C.
1785 E. Sahara Avenue, Suite 490
Las Vegas, NV 89104
Email: attorneycarrigan@amerilawyer.com

////

////

1 Nicolas W. Spigner
2 SPIEGEL & UTRERA, P.C.
3 8939 S. Sepulveda Blvd., Suite 400
4 Los Angeles, CA 90045
5 Email: attorneysigner@amerilawyer.com

Attorneys for Aaron Wallace

6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

/s/ Melina Hernandez